SPECIAL MEASURES FOR COVERT DATA COLLECTION: OVERSIGHT HANDBOOK

Editor: Predrag Petrovic

SPECIAL MEASURES FOR COVERT DATA COLLECTION: OVERSIGHT HANDBOOK

Editor: Predrag Petrovic

Belgrade
June 2015

SPECIAL MEASURES FOR COVERT DATA COLLECTION: OVERSIGHT HANDBOOK

Publisher
Belgrade Centre for Security Policy
Đure Jakšića 6/5, Belgrade
Phone: +381 (11) 3287-226
E-mail: office@bezbednost.org
Web: www.bezbednost.org

Authors
Predrag Petrovic
Sasa Djordjevic
Katarina Djokic
Jelena Pejic

Editor
Predrag Petrovic

Translation from Serbian
Ivan Kovanovic

Design and layout:
Marko Marinkovic

Print
UNAGRAF

Copies
100

ISBN
978-86-6237-106-5

CIP - Каталогизација у публикацији -
Народна библиотека Србије, Београд

342.738(497.11)
351.9:351.74/.75(497.11)
351.9:355.2(497.11)

SPECIAL Measures for Covert Data Collection: oversight handbook / [Predrag Petrović ... [et al.] ; editor Predrag Petrovic ; translation from Serbian Ivan Kovanovic]. - Belgrade : Belgrade center for security policy, 2015 (Beograd: Unagraf). - 82 str. : ilustr. ; 25 cm

Tiraž 100. - Napomene i bibliografske reference uz tekst. - Bibliografija: str. [81-82].

ISBN 978-86-6237-106-5
1. Petrović, Predrag, 1976- [аутор] [уредник]
a) Право на заштиту података о личности - Србија b) Безбедносни сектор - Надзор - Србија
COBISS.SR-ID 216105484

NORWEGIAN EMBASSY

Publication of this handbook was kindly supported by The Royal Norwegian Embassy in Belgrade, in the framework of the project "Who Controls the Wire: Towards the Effective External Oversight of the Use of Special Investigative Measures." The opinions expressed in the publication are solely those of the authors and do not necessarily reflect the positions of the Norwegian Ministry of Foreign Affairs.

Content

FOREWORD

Wiretapping and tailing of suspects are the traditional mainstays of security service activity. However, the multiplication and growing complexity of security threats and risks, as well as development of technology and communications has led to an increase in the number and variety of techniques used to covertly gather data, such as secretly accessing people's communications. Additionally, the number of government bodies and institutions implementing such measures has grown beyond the police and security services to include, for example, the Administration for the Prevention of Money Laundering and has also come to include private detective and investigative agencies. Today such measures are no longer applied only for preventative intelligence gathering but also in the course of criminal proceedings. The situation is further confounded by the fact that these activities are governed by a vast number of (unintegrated) regulations and by decreasing understanding of this field, both by the general public and by professionals. This is best illustrated by the fact that lawmakers use a variety of terms to define such measures in legislation: "special procedures and measures" (Law on the VBA and VOA), "special measures infringing on the privacy of correspondence and other communications" (Law on the BIA) and "special investigative activity" (Criminal Procedure Code).

The increasing number of covert data collection measures; the growing number of actors applying and approving them; the ever multiplying regulations governing their use and oversight; as well as disagreement on the terminology used to define them combine to make even basic understanding of these measures difficult. This publication aims to contribute to better understanding of this field as the basis for its more systematic and effective oversight. The first section of the handbook explains what special covert data collection measures are and what conditions are necessary for their application. The second section of the handbook is devoted to the various institutions authorised to deploy these measures in Serbia. This section also contains information on the different measures applied by various institutions, the legal conditions that must be met for their use and the actors tasked with their approval and oversight. The third section presents all of the institutions tasked with oversight and approval of these measures and reviews the powers available to them. The last section of the handbook lists the most important questions members of National Assembly committees for security sector oversight should be asking the security services and the judiciary in reviewing the use of covert data collection measures. Re-

sponses to these questions should yield information fundamental to the continued systematic oversight of this area.

The handbook is primarily aimed at the members of the National Assembly Security Services Control Committee and the Defence and Internal Affairs Committee, as their considerable security sector oversight powers put them in a position to make immediate use of this handbook. Furthermore, the handbook can also be of use to the interested public and organisations whose work intersects with these issues.

The handbook was created as part of the project, “Who Controls the Wire: Towards the Effective External Oversight of the Use of Special Investigative Measures”, but is founded on the many years of experience and specialised knowhow attained in this field by the BCSP team.

SPECIAL MEASURES FOR COVERT DATA COLLECTION

What are Special Measures for Covert Data Collection?

Special measures for covert data collection are defined as those methods of data collection that remain hidden from the persons, groups or organisations that are subject to investigation. All of these special measures can be divided into two main categories:

1. Those whose use has a lessened or negligible impact on human rights and freedoms. This group includes traditional operational measures such as interviewing the subject; covertly tailing or recording subjects; infiltration of groups and organisations; and accessing documents, public records or other data collection by public authorities. With the development of various forms of communication, there was an increase in the importance of public sources of data collection so the security services and police also collect and analyse data from the media, TV and the internet.

2. Those measures whose use significantly infringes upon human rights, particularly the right to privacy. These are usually measures that provide insight into the content of all forms of communication but also those measures that generate statistical data on past communications (i.e. access to stored data) and this category also includes covert domicile searches as one of the most aggressive special measures for covert data collection.

Who is authorised to use these special measures?

Use of special measures for covert data collection is an essential working tool for security services and the police, without which their work would be impossible to imagine. Over the past two decades, however, the number of bodies authorised to apply such measures has been on the rise and has come to include tax and customs authorities, agencies and administrative bodies for the prevention of money laundering, each of which has the power to apply certain special data collection measures. The reason behind this trend is twofold. First, there was a sharp increase in international (organised) crime, smuggling, tax evasion and money laundering, so there was a need to take measures to enable the investigation of these offences. Secondly, the aforementioned authorities are becoming more independent or less

dependent on the police and security services in conducting certain investigations.[1] The rapid rise of (organised) crime and industrial espionage,[2] combined with state security institutions' lack of resources to respond to these phenomena, has resulted in non-state organisations and private companies that provide security services (private investigation and detective agencies) gaining powers to apply certain measures of covert data collection. Laws[3] usually entitle private security companies to collect data via interviews, public records and other sources of public data, and also to tail subjects. It is not uncommon, however, for these companies to use significantly more intrusive methods in pursuit of profits, including wiretapping. This illegal practice has become possible due to the availability of affordable and accessible powerful listening devices and due to relatively loose government regulation of private security companies.

Why are these special measures applied?

State authorities have two main rationales for collecting data covertly. The first being to protect or advance national security or to prevent risks and threats to the security of the public, society and state institutions as well as, above all, the protection of the most vital economic and other interests of the society and the state. These threats can be the product of various individuals and groups (e.g. extremists, terrorists, etc.) both from within society and external to it. This involves collection of data and information on the activities, plans or intentions of various domestic and foreign state and non-state actors; the processing and analysis of said data; and its timely delivery to various users, primarily state officials, in order to enable them to make decisions correctly. Prevention is the key, therefore, as the primary goal is the interception of various threats to the interests of the state and society before they are realised. Data collection with this aim in mind is the fundamental *raison d'être* of security and intelligence services.

The second application of special measures is covert collection of data for the processing of a variety of (usually serious) criminal offences through the courts. This

1 See more in: Miroslav Hadžić and Predrag Petrović (Ed.), *Demokratski nadzor nad primenom posebnih ovlašćenja*, CCVO, Belgrade, 2008.

2 *How Real Is the Risk of Corporate Espionage Today?* Security Director's Report, Institute of Management & Administration, April 2009.

3 In Serbia it Law on Detective Activity, Art.10. 11. and 12.

kind of data collection is typical for police and other law enforcement bodies but also for the security services. Over the last two decades, however, due to increases in (international) organised crime and its links with terrorism, extremism and other security threats[4], the security services in some (mostly) transition states have come to be involved in the investigation of criminal offences. Other causes for this can be sought in the fact that these services descend from an authoritarian historical legacy, a characteristic of which is that security services perform a significant quantity of police work (hence the term secret police).

There has, however, been a reverse trend which sees police structures implementing special measures aimed at prevention of organised crime. Some states have, therefore, established special units within police structures while others have formed special, independent police agencies with the aim of preventatively collecting data on the activities and intentions of organised crime groups (e.g. the British National Crime Agency).

Today, at a time of rapid, global expansion of private companies that provide security services, it is worth discussing a third, commercial purpose behind data collection that sees private security companies collecting data on behalf of the private citizens and governmental clients who award them contracts. The services on offer are diverse and include verification of spouse fidelity; finding missing persons and property; gathering forensic evidence; counterintelligence and security protection for companies and businesses; commercial viability checks and similar. Over the last decade there has been a trend, led by Western states, of government authorities engaging private intelligence gathering agencies o collect all kinds of data relating to national security.[5]

4 Frank G. Madsen, *Transnational Organized Crime*, Routledge, London, 2009, pp. 62-80.

5 Patrick M. Skinner, This Disaster Happened Because the CIA Outsourced Accountability, TIME, December 10, 2014, internet: http://time.com/3627834/torture-report-cia-contractors/, app.: 10.02.2015.

Who authorises the application of special measures?

Special measures for covert data collection that have a lower impact on human rights (e.g. secret surveillance in public spaces) can be authorised by the heads of intelligence and security services or police chiefs, as well as public prosecutors (in the case of controlled delivery)[6]. However, the application of special measures that have a more significant impact on human rights (such as covert communications monitoring) require authorisation by an independent body other than the body applying the measures, most often a court. In this eventuality the security or intelligence service and the public prosecutor (if the application of special measures is related to criminal proceedings) propose the application of such measures and then seek written judicial approval. [7]

A PROPOSAL FOR APPLICATION OF SPECIAL MEASURES MUST INCLUDE:

- The type of measure to be applied
- Available information on the individual, group or organisation subject to the special measures
- Compliance with conditions on the application of special measures (reasonable suspicion)
- The scope of measures and the location of their application
- The timeframe for application

DETERMINATION OF SPECIAL MEASURES TO BE USED INCLUDES:

- The type of measure
- Available information on the individual, group or organisation subject to the special measures
- Compliance with conditions on the application of special measures (reasonable suspicion)
- Method of application
- Scope and timeframe for application

6 The Criminal Procedure Code, Art. 181., Law on Military Security Agency and Military Intelligence Agency Art. 13., Law on the Security-Information Agency Art. 9.

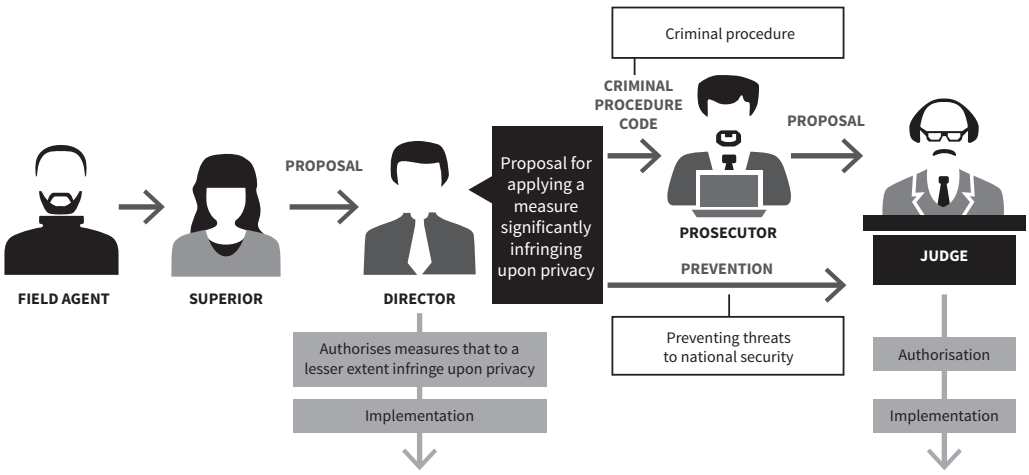
7 See: The criminal procedure law Art. 145, "Special Investigative Activities" Art.161-187, Art. 286; Law on Military Security Agency and Military Intelligence Agency Art. 13a-14; Law on the Security-Information Agency Art. 15-15a.

Less stringent legal standards apply for the use of special measures by private investigators and detective agencies as they are legally only authorised to make use of less intrusive measures. These agencies, therefore, only require written authorisation on the part of their clients to apply data collection measures. These agencies then submit requests for information to the relevant bodies/institutions (e.g. hospitals). Private companies and agencies must, of course, be registered and licensed to conduct such investigative activities and their employees must have special identification for that purpose[8].

DATA ACCESS REQUESTS FOR PRIVATE DETECTIVE AGENCIES MUST CONTAIN:

- The name and address of the registered agency;
- The type of data sought;
- A commencement date for processing, i.e. they must specify which data is being collected;
- A reason for seeking access (justification);
- The legal foundation for granting access (authorisation by the client);
- The name and address of the client.

Image 1: Flow chart showing process of recommending and approving measures applied by the security services



8 Law on Detective Activity, Art. 13.

Conditions for the application of special measures

Given that special measures of this kind are a covert and exceptionally intrusive means of data collection, certain conditions must be fulfilled for their application:

- The measures should be clearly defined and lawful;
- There should be a clearly prescribed procedure for their approval, oversight and supervision;
- Principles of independent oversight and approval must be maintained;
- The special measures applied should be necessary and proportionate.[9]

For the application of special measures to be valid, they must be clearly defined by primary, rather than secondary, legislation. This implies that the special measures must be sanctioned, the conditions for their application and the procedures for their approval clearly defined and the oversight body clearly determined. It is also important that approval of measures is carried out independently, that the body proposing the implementation of special measures is separate from the body that approves their use. Furthermore, the body that approves the use of special measures significantly impacting human rights (secret communications tapping, etc.) must be also be other than the body that proposes their use, in most cases this is a court.

In addition to meeting these formal principles and conditions, it is also of great importance that the essential conditions for their use be met. Principally, it is necessary for there to be reasonable suspicion that the targeted person, group or organisation is involved in activity that threatens the security or interests of the state and of society or is otherwise commissioning or has already committed a serious crime. Secondly, it is important that these offences cannot, without causing undue difficulties, be detected, prevented or proven using means other than special investigative measures. In practice, this means that the security services and police cannot gather evidence in any other way or that the investigation would be delayed if other means are used. It is important, therefore, that the application of special investigative measures is necessary or that only through their application can a legitimate interest or goal be protected or realised.

9 See: Criminal Procedure Code, art. 161., Law on the Security-Information Agency, Art 14.

For the proper use of these measures, however, it is not only important that their application is deemed necessary but that they are applied in proportion to the goal sought. Thus, it should always be determined whether the specific measure applied (and not all measures in general) will lead to the successful realisation of the goal or whether the objective can also be reached by application of other measures less restrictive to human rights. Also, the application of special investigative measures should not extend to other entities; neither should their use be prolonged without valid justification. Moreover, as a rule the application of special investigative measures must cease prior to the deadline set for their use or upon achieving the purpose for which they were applied.

Reasonable suspicion *reflects a set of evidence – i.e. facts and circumstances – which suggests that a person, group or organisation is preparing acts directed against the security and interests of the state and of society, or are otherwise in the process of commissioning a serious crime. Reasonable suspicion is the starting point of an investigation by state authorities and must not, therefore, be mere conjecture or speculation but should contain a degree of likelihood. It must be based on at least two sources, indicating that the relevant actors are possible security threats or offenders. If we take high-risk events as an example, general suspicion would be that there will be incidents at a Serbia vs. Albania football match. Reasonable suspicion would, in this case, be specific information (obtained through operational activities) that some persons are preparing an incident using a drone, which would justify the application of specific measures to counter this threat.*

The Most Common Errors in Authorisation of Special Measures

For unconsolidated democracies with extremely weak institutions (particularly the judiciary) it is not uncommon for frequent errors to occur in the approval of special investigative measures.[10] This results in unjustified violations of the human rights of persons who are, without a valid basis, targeted by special investigative measures. If the purpose of the special investigative measures is to collect evidence of criminal activity, errors in their approval can lead to their being inadmissible in court and can jeopardise the outcome of the case. Errors in the approval of special investigative measures are manifold:

- Errors in the form and content of orders requesting special investigative measures;
- Incorrect assessment of 'reasonable suspicion',
- Incorrect assessment of the necessity or proportionality of certain measures for the successful conclusion of the investigation (it may not have been necessary to apply special measures or it may have been necessary to apply other measures);
- Incorrect calculation of deadlines for the expiry of special measures.

Hence, it is of critical importance that all bodies involved in processes of recommendation, approval and oversight ensure, in as much detail as is possible, that all aforementioned conditions are met, not only for the application of special investigative measures in general but also for each specific measure.

Who Oversees and Reviews the Application of Measures?

As has been mentioned, the courts are, for a number of reasons, the most important institution that can exercise oversight and review the application of special measures. Firstly, the courts approve measures and can deny their application if the statutory requirements are not met. They can also order the destruction of materials collected through the application of these measures if criminal proceedings are dropped or if the measures were not applied in accordance with the law. Finally, the security services and police are obliged to submit reports to the courts about applied measures and evidence gathered through their application – or earlier if so

10 Read more: Silvija Panović-Đurić, *Primena specijalnih istražnih sredstava*, Council of Europe Office in Belgrade, Belgrade, 2013.

requested by the court.[11] The Ombudsman and the Commissioner for Information of Public Importance and Personal Data Protection can initiate a review of the legality and propriety of special investigative measures if they receive a request to do so from members of the public or independently (*ex officio*) if they become aware of human rights violations. Representatives of both institutions have access to information classified at the highest level ("state secret") for which they are cleared through security checks.

On the other hand, the National Assembly's Security Services Control Committee is authorised to exercise *post factum* oversight of the implementation of special investigative measures. The primary aim of this type of control is the elimination of systematic weaknesses and legal irregularities by amendment of procedures and regulations, if these are found wanting.[12]

Furthermore, all bodies able to apply special measures (security services or police) have their own internal affairs departments that, in spite of being a form of 'self-control', are actually the first line of defence of the integrity of these institutions. In Serbia, however, these internal control mechanisms are underdeveloped and produce only very modest results.

11 In case of three types of special measures. See more in the chapter Judicial Review.

12 Parliamentary oversight of the security services is currently regulated in detail by a decision, which is non-binding for future convocations, as the Rules of Procedure do not foresee that committees adopt own regulation. See: National Assembly of the Republic of Serbia – Security Services Control Committee "Decision Regulating Direct Oversight of the Security Services in Accordance with the Law Regulating the Basic Organisation of the Security Services of the Republic of Serbia, the Laws on the Security Services and the Rules of Procedure of the National Assembly. Number 02-1322/13" Belgrade, 29 March 2013.

AGENCIES APPLYING SPECIAL MEASURES

The Security-Information Agency

The Security-Information Agency (BIA) is a civilian, national and central security service of the Republic of Serbia. Its responsibilities define it as a 'mixed' type of security service due to the fact that it carries out both intelligence and counter-intelligence tasks but also functions as a security service. Additionally, when performing some tasks, BIA operatives are authorised to apply police-like powers, including the right of arrest. These tasks include detection, monitoring, prevention and interdiction of the activities of organisations and persons engaging in organised crime and criminal acts linked to foreign and domestic terrorism, crimes against humanity, breaches of international law and also threats to the constitutional order and the security of the Republic of Serbia.[13] The Director of the BIA is appointed and discharged by the Government.[14]

The BIA applies covert data collection measures preventatively, in order to counter national security threats but also to prosecute criminal acts through the courts. The special measures, determined by the Criminal Law Code, which the BIA applies, are presented on page 33.

13 Law on the Security-Information Agency Art. 2.

14 Law on the Security-Information Agency Art. 5.

Table 1: Security-Information Agency - Measures Authorised by Courts

Legal Framework	**Law on Security-Information Agency**
Measures:	1. covert surveillance and communications tapping regardless of the technology used or the electronic/real-world address; 2. covert surveillance and communications tapping in public places and places where access is restricted or in internal spaces; 3. statistical electronic surveillance of communications and information systems with the aim of collecting data on communications or locations where mobile technology has been used; 4. computer searches of processed personal and other information and comparative analysis with data collected using the aforementioned means; 5. covert surveillance and recording of locations, premises and objects, including equipment for automatic data processing and equipment that stores or can store electronic records.
Approved by:	Applied on proposal by the Director of the BIA and approved by the President of the Belgrade High Court, or a judge selected from that court's Special Department for Combating Organised Crime.
Duration:	3 months, which can be extended by a further 3 months a maximum of three times
Applied in cases of:	Threats to the national security of the Republic of Serbia
Application overseen by:	The respective courts are not authorised to exercise oversight of the application of these measures nor is the BIA obliged to submit reports on how the measures are applied
What happens to the information that is collected?	Upon conclusion of the investigation the BIA is not required by law to destroy data collected by the application of these measures.

Table 2: Security-Information Agency - Measures Authorised by Director

Legal Framework:	**Covert Regulative Legislation Passed by the Director of the BIA**
Measures:	• covert search of premises, belongings and objects; • covert cooperation • covert surveillance and monitoring
Approved by:	The Director of the BIA
Duration	--
Applied in cases of:	Threats to the security of the Republic of Serbia or according to the needs of criminal investigations
Application overseen by:	Self-control by the BIA

The Military Security Agency

The Military Security Agency (VBA) is responsible for security, counter-intelligence and counter-terrorism relating to the Serbian Armed Forces and the Ministry of Defence. As part of its counter-intelligence functions, among other things, the VBA employs detection, investigation and documentation of criminal offences committed against the constitutional order and security of the Republic of Serbia, as well as crimes against humanity and international law and also the most serious criminal offences linked to organised crime. Similar to the BIA, the VBA and its operatives engaged in the aforementioned activities, can apply police-like powers but not the power of arrest. The VBA is part of the Ministry of Defence.[15] The VBA Director and deputy director are appointed by the President of the Republic on the proposal of the Minister of Defence if the candidate is a civilian. The Director answers to the Minister of Defence.

Measures of covert data collection are applied by the VBA preventatively but also to prosecute through the courts those offences committed within the Ministry of Defence and the Serbian Armed Forces. Measures applied by the VBA according to the Criminal Law Code are presented on page 33 of this handbook.

The VBA is authorised to apply measures of covert data collection on employees of the Ministry of Defence and the Serbian Armed Forces. When the VBA, in conducting these tasks as part of its operations, assesses that these measures should also be applied to other persons, it must immediately notify the Security-Information Agency or the police in order to determine the best way to proceed.[16]

15 Law on Military Security Agency and Military Intelligence Agency, Art. 2. and 5.

16 Law on Military Security Agency and Military Intelligence Agency, Art 6,para.3.

Table 3: Military Security Agency - Measures Authorised by Courts

Legal Framework:	**Law on the Military Security Agency and the Military Intelligence Agency**
Measures:	1. covert electronic surveillance of telecommunications and information systems in order to gather data on communications traffic, without access to the contents; 2. covert recording and documentation of conversations in public and closed spaces, using technical equipment; 3. covert surveillance of the content of letters and other communication, including covert electronic surveillance of the content of telecommunications and information systems; 4. covert surveillance and recording of internal spaces, closed premises and objects.
Approved by:	On proposal by the Director of the VBA, measure 1 is approved by a high court within the appeals court in the region where it is applied or within which the action being detected, monitored and prevented by the VBA. These could be high courts in Novi Sad, Belgrade, Kragujevac and Niš. On proposal by the Director of the VBA, measures 2 to 4 are approved by the Supreme Court of Cassation, as authorised by the presiding judge of that court.
Duration:	6 months, this can be extended by a further 6 months.
Applied in cases of:	Security threats directed against the Ministry of Defence and the Serbian Armed Forces.
Application overseen by:	The courts cannot review application of these measures, neither is the VBA obliged to submit reports on the application of these measures.
What happens to the information that is collected?	Once the investigation is concluded, the VBA is not required by law to destroy data gathered by application of these measures.
Note:	The VBA is authorised to apply covert data collection measures exclusively on employees of the Ministry of Defence and members of the Serbian Armed Forces. If, in the course of an investigation, the VBA assesses that covert data collection measures should be applied to other persons, it is obliged to immediately inform the Security-Information Agency or the police, in order to determine a course of action.

Table 4: Military Security Agency - Measures Authorised by the Director

Legal Framework:	**Law on the Military Security Agency and the Military Intelligence Agency**
Measures:	1. operational infiltration of organisations, groups or institutions; 2. covert gathering and acquisition of documents or objects; 3. covert access to databases, in accordance with the law; 4. covert tailing and surveillance of persons in open spaces and public places, with use of technical equipment; 5. covert use of services provided by persons or businesses with compensation (article 22, item 4)
Approved by:	The Director of the VBA
Duration:	--
Applied in cases of:	Security threats directed against the Ministry of Defence and the Serbian Armed Forces.
Application overseen by:	Self-control – the VBA Internal Control department and the Inspector General of the VBA and VOA

The Military Intelligence Agency

The Military Intelligence Agency (VOA) is authorised to collect, analyse, assess and provide data and information (of a military, military-political, military-economic, scientific and technological nature) relating to potential and present threats, activities, plans or intentions of foreign states and their armed forces, international and foreign organisations, groups and individuals that are directed against the Ministry of Defence, the Serbian Armed Forces, the sovereignty, territorial integrity and defence of the Republic of Serbia.[17] The VOA is part of the Ministry of Defence. The Director of the VOA and the deputy directors are appointed and discharged by the President of the Republic on recommendation by the Minister of Defence if the candidates are professional soldiers or by the Government, on recommendation of the Minister of Defence, if the candidates are civilians. The Director answers to the Minister of Defence.

The VOA is authorised to apply all special procedures and measures other than covert optical-electronic monitoring of persons and communications.

Table 5: The Military Intelligence Agency - Measures Approved by the Director of the VOA

Legal Framework:	**Law on the Military Security Agency and the Military Intelligence Agency**
Approved by:	The Director of the VOA or persons authorised by the Director
Duration:	As long there is a rationale for their application
Applied in cases of:	Data and information on potential and present dangers, activities, plans and intentions of foreign states and their armed forces, international organisations, groups and individuals.
Application overseen by:	Self-control – Internal Control department of the VOA and the Inspector General of the VBA and VOA
What happens to the information that is collected?	Once the investigation is concluded, the VOA is not required by law to destroy data gathered through the application of these measures
Note:	The VOA is not authorised to apply measures of covert data collection that significantly impact the privacy of members of the public (e.g. covert electronic surveillance of telecommunications)

17 Law on Military Security Agency and Military Intelligence Agency, Art. 24-25.

The Police

The police are the most conspicuous state body responsible for maintaining security in society. The complexity of criminal and corruption investigations requires the police to infringe on individuals' right to privacy, including their private home or family lives and correspondence. Today police work is more than ever founded on covert gathering, processing and use of data to combat security threats. In most countries, including in Serbia, the police are legally empowered to apply measures of covert data collection in the event that it is not possible to gather information on the workings of criminal groups. As a result, police work increasingly requires the use of informants, the monitoring and interception of telephone conversations and internet communication or the interception of suspicious shipments that are then deliberately allowed to reach their destinations.

In Serbia there are several separate units authorised to conduct secret investigations: the Criminal Force Directorate, the Internal Affairs Sector and the Security Affairs Department within the Office of the Minister of Interior (MoI).

THE CRIMINAL FORCE DIRECTORATE

The Criminal Force Directorate is the department within the police responsible for detecting and combating crime. Members of the Criminal Force Directorate may, in order to detect offences, apply special evidence gathering techniques and other measures of covert data collection in accordance with the Constitution, the Law on the Police, the Criminal Law Code and the Law on Electronic Communication. Specialised units within the Directorate are responsible for applying and coordinating the application of measures for covert data collection: the Special Investigative Methods Service, the Department for Observation and Documentation and the Department for Undercover Investigators.[18]

18 The Law on Police, Art. 71

THE INTERNAL AFFAIRS SECTOR

The Internal Affairs Sector is tasked with investigation of crimes and corruption within the police and ensuring the legality of police work. Members of the Sector are authorised to apply all police powers, including measures of covert data collection. According to the Criminal Procedure Code, members of the Section for Covert Audio and Optical Surveillance of Suspects within the Department for Criminal-Operational Affairs of the Internal Affairs Sector are tasked with special investigative activities as well as other covert data collection measures[19].

THE SECURITY AFFAIRS DEPARTMENT

The Security Affairs Department is seconded to the Office of the Minister of Interior. It is tasked with securing the MoI and protecting classified data. In conducting its activities it is authorised to apply operational methods prescribed by Criminal Procedure Code and the Law on the Police, these include covert data collection measures. The aim is to ensure the security of certain buildings, persons and police functionaries. Providing security involves the use of counter-intelligence to thwart terrorist, extremist, intelligence and other subversive activities by foreign intelligence services, organisations and individuals directed against the Minister of Internal Affairs.

WHICH SPECIAL MEASURES CAN THE POLICE APPLY?

The police can apply ten special data collection measures: (1) surveillance of suspicious transactions, (2) covert communications monitoring, (3) covert tailing and recording, (4) simulated business activity, (5) computer data searches, (6) controlled delivery, (7) undercover agents, (8) acquiring records of telephone conversations, accessed databases and data on locations where communications have taken place, (9) police observation, (10) measures relating to targeted pursuit.

Measures 1-8 are defined by the Criminal Procedure Code and are presented on page 33 of this handbook.

19 Information booklet about work of Ministry of Interior (in Serbian), updated 25.12.2013.god. p. 12.-14. available on http://www.mup.gov.rs/cms/resursi.nsf/INFORMATOR%20maj%202015%20LATINICA.pdf

Table 6: Police Measures that authorised police officers may apply on own initiative

Legal Framework	**Law on the Police**
Measure	**Police Surveillance***
Approved by:	Authorised police officers may implement police surveillance on their own initiative, on orders by the superior or as instructed by a competent authority.**
Duration:	Unlimited
Reason for application:	Combating crime
Application overseen by:	–
What happens to the information that is collected?	Used in operations or as evidence
Note:	Surveillance is conducted in public and other accessible places without encroaching on the right to privacy.

* The Law on Police, Art. 71
** The Law on Police, Art. 31. para. 3.

Table 7: Police - Measures Approved by the General Police Director

Legal Framework	**Law on the Police**
Measure	Targeted pursuit*
Approved by:	The President of the High Court of Cassation can, on recommendation by the General Police Director, authorises the application of special investigative activities defined by the Criminal Procedure Code in order to ensure the apprehension and arrest of persons suspected of serious criminal offences or if an international arrest warrant is in force.
Duration:	Six months. Can be extended by a further six months.
Reason for application:	Combating crime
Application overseen by:	High Court of Cassation
What happens to the information that is collected?	The High Court of Cassation, or rather an authorised judge, is required to destroy gathered information and to record its destruction.
Note:	This measure is applied when the police is unable to apprehend and arrest the suspect through other means. Data gathered through targeted pursuit cannot be used as evidence in criminal proceedings.
* The Law on Police, Art. 83.	

Criminal Procedure Code

Table 8: Criminal Procedure Code – Measures Authorised by Court

Measures:	Special investigative activities:* • 1) covert communications monitoring • 2) covert tailing and recording • 3) simulated business activity • 4) computer data search • 5) engagement of undercover agents Other special measures for covert data collection • 6) surveillance of suspicious transactions (Article 145) • 7) acquiring records of telephone conversations, accessed databases and data on locations where communications have taken place (Article 286, Items 3-5)
Approved by:	The judge presiding over the case, on recommendation by the public prosecutor.
Applied by:	The police, the Security-Information Agency, the Military Intelligence Agency,
Duration:	In the case of computer data searches, these measures can be applied by tax, customs and other services and authorities as well as legal entities so authorised.
Reason for application:	3 months, which can be extended by a further 3 months a maximum of three times
Application overseen by:	State bodies applying these measures are required to keep daily reports on their application, which are then submitted to the presiding judge and the public prosecutor on their request. Upon conclusion of measures' application, the relevant government body submits to the presiding judge recordings of communications, correspondence and other items along with a special report containing the following: the start and end date of the monitoring; details of the official who conducted the monitoring; a description of technical equipment used; the data collected and an evaluation of the operations applicability and its results.
What happens to the information that is collected?	Gathered data are used as evidence in criminal proceedings against the suspect. In the event that criminal proceedings are not initiated by the public prosecutor within six months of becoming aware of the gathered data or if it is announced that the data will not be used in the proceedings, the judge presiding over preliminary proceedings shall issue a decision on the destruction of the material. In the event that the data were not gathered in accordance with regulations, they cannot be submitted as evidence, in other words, they cannot affect the judge's deliberation. Unlawful evidence is struck from records, sealed and retained by the judge presiding over preliminary proceedings until criminal proceedings are legally concluded, at which time it is destroyed and its destruction is recorded. If proceedings are initiated on the basis of unlawfully gathered data, the unlawful data are retained until the criminal proceedings are legally concluded.
* Criminal Procedure Code, Art. 161.-187.	

Table 9: Criminal Procedure Code - Measures Authorised by the Public Prosecutor

Measure	Controlled Delivery
Approved by:	The Prosecutor's Office for Organised Crime (or for War Crimes) can, in order to gather evidence on and detection of suspects, authorise an illegal or suspect package to be delivered within Serbia or to enter, exit or traverse the country's borders.
Duration:	Until the package is delivered.
Reason for application:	Combating crime
Application overseen by:	In conducting a controlled delivery the police submit a report to the public prosecutor containing: information on the start and end date of the delivery; details of the official conducting the operation; a description of technical equipment used; information on the persons affected and the results of the operation.
What happens to the information that is collected?	Collected material is not destroyed.
Note:	Controlled delivery is conducted with the consent of affected countries, in accordance with ratified international treaties.
Measure	**Acquiring Data from Financial Institutions (Article 144)**
Approved by:	The Public Prosecutor can order banks or other financial institutions to, within a given deadline, submit data on the accounts of a suspect, if they exist.
Duration:	–
Reason for application:	Combating crime
Application overseen by:	The Public Prosecutor
What happens to the information that is collected?	The Public Prosecutor destroys the gathered data within six months of becoming aware of the data if criminal proceedings are not initiated, if the prosecutor will not request proceedings or if the data is not deemed necessary for proceedings.

The Administration for the Prevention of Money Laundering

The Administration for the Prevention of Money Laundering (hereafter, the Administration) is a financial intelligence service within the Ministry of Finance. It is tasked with tracking suspicious transactions and persons, on which it reports to the relevant government department in cases of possible money laundering and the financing of terrorism.[20] The Administration tracks suspicious transactions or persons and gathers data from the *obligor*, a term that denotes all actors within the financial and other sectors who conduct financial transactions (banks, registered exchange bureaus, audit companies, etc.).[21] In addition to the obligor, lawyers are also legally obliged to apply measures for the detection and prevention of money laundering and the financing of terrorism, in other words they must inform the Administration about suspicious persons and transactions.[22] Obligors and lawyers are prohibited from alerting their clients to the fact that the Administration is accessing their data. In this sense, it can be concluded that the Administration applies covert data collection measures. As this is not, however, legally codified, external oversight over the implementation of these measures is limited.

The Administration applies two measures that can be characterised as special investigative measures.

20 Law on the Prevention of Money Laundering and Financing Terrorism, Article 52

21 Obligors are defined by the Law on the Prevention of Money Laundering and Financing Terrorism, Article 4

22 Ibid. Article 5. Even after the December 2014 amendments, the Law on the Prevention of Money Laundering and Financing Terrorism does not require public notaries to gather such data (Law on the Prevention of Money Laundering and Financing Terrorism, Official Gazette of the Republic of Serbia, Nos. 91/2010 from 03/12/2010)

Table 10: Special Measures Applied by the Administration for the Prevention of Money Laundering

Legal foundation	Law on the Prevention of Money Laundering and Financing of Terrorism
Measure:	**1) accessing data from obligors and lawyers**
Approved by:	The Director of the Administration
Duration:	Not defined
Reason for application:	If the Administration assesses that there is reasonable suspicion of money laundering or the financing of terrorism regarding certain transactions or persons
Application overseen by:	Prior to application: The relevant Administration officials and the Director After application: Possible investigation by the Ministry of Finance inspectorate. The Administration submits an annual report to the Government
What happens to the information that is collected?	The Administration analyses the gathered data, which can be submitted to other Serbian government bodies or, under legally defined conditions, to the government bodies responsible for preventing money laundering or the financing of terrorism from other countries.
Note:	Obligors are required by law to report to the Administration financial transactions amounting to 15,000 euros, as well as regarding every client or transaction they suspect may involve money laundering or the financing of terrorism.* The Administration may also request data on transactions or persons that are deemed suspicious. The Administration is required by law to request data not only on persons suspected of money laundering or the financing of terrorism but also on persons who are linked to them through business or financial transactions** Obligors and lawyers are required to store data or documentation on transactions or clients for at least ten years from the contact with the client or from the completed transaction.***
Measure:	**2) tracking the financial operations of legal entities or persons****
Approved by:	The Director of the Administration
Duration:	3 months from the issuing of a warrant
Reason for application:	If the Administration assesses that there is reasonable suspicion of money laundering or the financing of terrorism regarding certain transactions or persons.
Application overseen by:	Prior to application: The relevant Administration officials and the Director After application: Possible investigation by the Ministry of Finance inspectorate. The Administration submits an annual report to the Government.
What happens to the information that is collected?	The Administration analyses the gathered data, which can be submitted to other Serbian government bodies or, under legally defined conditions, to the government bodies responsible for preventing money laundering or the financing of terrorism from other countries.
Note:	A tracking order can also cover persons who have had business dealings or financial transactions with the suspect. *****

* Law on the Prevention of Money Laundering and Financing Terrorism, Article 9
** Law on the Prevention of Money Laundering and Financing Terrorism, Article 53, Item 2
*** Ibid, Article 77, Item 1
**** Law on the Prevention of Money Laundering and Financing Terrorism, Article 57.
***** Ibid, Article 57, Item 2. The Administration, however, does not have details indicating that it used these powers in the period 2010 to 30/09/2014. (The Administration for the Prevention of Money Laundering. Response to BCSP questionnaire, 04/11/2014)

What Private Investigators Can and Cannot Do

Private investigators (individuals or legal entities engaging in private investigations) are explicitly, legally prohibited from applying "operational methods and means and operational technical equipment, applied by the authorities on the basis of special regulations". In practice, however, observing or proving that private investigators illegally gathered data is difficult. The Ministry of Interior should be required by law to investigate the activities of private agencies and to issue fines of 100,000 to 1,000,000 dinars for the unauthorised application of operational methods and means. There are, however, suspicions that private investigators apply these methods (for example, covert communications monitoring, i.e. wire-tapping) regardless of their legal prohibition.[23]

On the other hand, private investigators can gather and process personal data in accordance with regulations governing the protection of personal data and freedom of information. This means that private investigators can process data without the consent of the person whom the data regards, but only in accordance with the Law on Personal Data Protection.

WHAT DOES THE LAW ON PERSONAL DATA PROTECTION SAY ABOUT UNSOLICITED DATA PROCESSING?

Article 12**

Processing without consent shall be allowed in the following cases:

1) To achieve or protect vital interests of the data subject or a third party, in particular their life, health and physical integrity;
2) For the purpose of discharging duties laid down by a law, an enactment adopted pursuant to a law or a contract concluded between the person concerned and the controller, as well as for the purpose of contract preparation (processing data of a third person is unlawful);
2ª) in order to raise funds for humanitarian purposes;
3) In other cases envisaged by this Law or another regulation adopted pursuant to this Law, for the purpose of achieving a prevailing justifiable interest of the person concerned, the controller or a user.

23 Gedošević, L. "Sabić says Serbian citizens have been phone tapped by the State and private 'services'" (Serbian „Šabić: Građane u Srbiji prisluškuju i državne i privatne 'službe'"), Blic Online, 02/05/2013: http://www.blic.rs/Vesti/Drustvo/380665/Sabic-Gradjane-u-Srbiji-prisluskuju-i-drzavne-i-privatne-sluzbe

The Law on Private Investigators outlines the types of data state bodies, legal entities and other database operators are required to hand over to private investigators. These are data on:

1. the person's residence or domicile;
2. motor vehicle and boat ownership;
3. insurance policies;
4. real estate ownership;
5. pension and disability insurance;
6. data from court records in cases when the user is so authorised;
7. data from government archives.

In order to gain access to these data, investigators must submit a request to those in possession of the data (e.g. a government body), which contains the following:

1. the name and address of the legal entity or private investigation agency;
2. the type of data requested;
3. the start date for processing or accessing the data;
4. justification for accessing the data;
5. the legal basis for processing the data (the user's legal authority);
6. the name and address of the user.

Those in possession of the data are required to refuse requests for data that are, according to regulations on data classification, defined as classified.

OVERSIGHT OF THE APPLICATION OF SPECIAL INVESTIGATIVE MEASURES

Judicial Review

Judicial review and oversight is carried out in accordance with two legislative regimes governing the implementation of special investigative measures: the Criminal Procedure Code (CPC) or legislation specific to the relevant service (the Law on the Security-Information Agency and the Law on the Military Security Agency and the Military Intelligence Agency), when security services apply these measures in the course of their operations or preventatively. The form and scope of judicial review depends on which legislative regime the measures are applied under. Additionally, judicial review and oversight can be carried out in three phases: before the measures are applied; in the course of the measures' application; and after the completion of the measures' application. Review of measures implemented in accordance with the Criminal Procedure Code is, in that sense, comprehensive as it covers all three phases. On the other hand, review of measures applied in accordance with laws on the security services is almost wholly limited to the first phase (review prior to application).

THE CRIMINAL PROCEDURE CODE

The Criminal Procedure Code provides for judicial review and oversight of special evidence gathering activities prior to their application (*ex ante*) and upon the completion of their application (*post factum*). Oversight of certain evidence gathering activities can be conducted during their application. This level of review and oversight is not surprising, since evidence gathered unlawfully is inadmissible in court.

Ex Ante Review:

Ex ante review is carried out through approval of special evidence gathering activity. Most special evidence gathering procedures are determined by the judge presiding over preliminary proceedings, on the request of the public prosecutor. A judicial warrant must be justified and the CPC clearly prescribes what this justification must contain. On the other hand, controlled delivery is determined directly by public prosecutors.

Courts or prosecutors must also conduct *ex ante* review of the application of certain activities not recognised as special evidence gathering activity by the CPC but the application of which significantly infringes the right to privacy. On request by the

prosecutor, judges presiding over preliminary proceedings can, therefore, approve surveillance of suspect transactions and access to phone records, base stations used or locations from which communications were conducted. Prosecutors can approve access to data from banks and other financial institutions in accordance with Article 144 of the CPC.

Table 11: Who authorises special investigative activities

Requested by the public prosecutor, approved by the judge presiding over preliminary proceedings*	• Covert communications monitoring (including further expansion, in accordance with Article 169); covert tailing and recording; simulated business activity; computer data searches; engagement of undercover agents • Monitoring of suspicious transactions; • Access to phone records, base stations used or locations from which communications were conducted
Determined by the public prosecutor	• Controlled delivery; • Access to data from banks and other financial institutions in accordance with Article 144 of the CPC
* Since 2013, the concept of prosecutorial investigation has been available in Serbia. So far, however, due to numerous problems, prosecutorial investigation has not taken off in practice (see: Karović, B. "Prosecutorial Investigation Delayed." (Serbian: „Tužilačka istraga zakočena"), Danas Today, http://goo.gl/KhDH21). This indicates that measures are de facto proposed by the police and security services, with prosecutors only passing these proposals to judges presiding over preliminary proceedings.	

Review During Application:

The judge presiding over preliminary proceedings and the public prosecutor have the power to oversee implementation of some special evidence gathering activities during their application. This applies to the following measures: covert communications monitoring; covert tailing and recording and simulated business activity. Government agencies tasked with any of these activities are required to produce daily reports on their application. These daily reports, together with supporting materials defined by the CPC (for example, recordings made in the course of the operation) are submitted to the preliminary proceedings judge and the public prosecutor, however, the submission of these materials is not automatic and they must be requested. It is not known how frequently judges make use of this power.

Table 12: The possibility of judicial review by phase of application

Measure	*Ex ante* review	Review during application*	*Post festum* review**
Covert communications monitoring	Yes	Yes	Yes
Covert tailing and recording	Yes	Yes	Yes
Simulated business activity	Yes	No	Yes
Controlled delivery	Prosecutor oversight only	No	Yes
Engagement of undercover agents	Yes	No*	Yes
Access to phone records, base stations used or locations from which communications were conducted	Yes	No	(The police report to the public prosecutor on applying this measure but do not report to the judge who approved the measure)
Access to data (from banks and other financial institutions)	Exclusively by the prosecutor	No	No
Monitoring of suspicious transactions	Prosecutor oversight only	No	No
Nadzor sumnjivih transakcija	Yes	No	No

* If the measure is reviewed by the same body that approved it.
** If the measure is reviewed by the same body that approved it.

Post Factum Review:

Upon concluding a special evidence gathering operation, the government agency tasked with its implementation, is required to report on the operation and any collected materials (recordings, documents) to the judge presiding over preliminary proceedings. In the event of a controlled delivery, the report is submitted to the public prosecutor. The contents of reports for each type of operation are clearly specified. As a rule, reports should include information on the when the operation was undertaken, details of who conducted it and the results of its application. For covert communication monitoring and covert tailing and recording the report must contain an assessment of whether applying these evidence gathering operations was appropriate. On the other hand, police engaging in operations to access phone records, base stations used or locations from which communications were conducted must

inform the public prosecutor but the CPC does not prescribe any requirement to report to the judge presiding over preliminary proceedings who approved the application of the measure.

Materials collected in special evidence gathering operations that will not be used in criminal proceedings is destroyed on the order of, and under the supervision of, the judge presiding over preliminary proceedings. The judge can (but isn't required to) inform the person whose communications were subject to covert monitoring, provided this would not affect the likelihood of criminal proceedings being initiated. The same applies to data collected from banks and other financial institutions or to the tracking of suspicious transactions (all of which are destroyed on the decision of the public prosecutor). The entity that was subject to evidence gathering operations must be informed of this by the judge (in cases of the monitoring of suspicious transactions) or the public prosecutor (in cases of the accessing of data). It must, however, be noted that in cases of covert tailing and recording and computer searches, the CPC does not envisage the possibility of persons 'subject to measures' being notified. Finally, when it comes to measures named in Article 286, the CPC prescribes that those subject to the measures can file a complaint with the judge presiding over preliminary proceedings. It is not, however, clear how the subject would even become aware that they are subject to such measures.

Evidence gathered unlawfully through these special procedures is inadmissible in court and must be treated in the same way as other unlawful evidence: sealed and retained by the judge presiding over preliminary proceedings until the final completion of criminal proceedings, whereupon it must be destroyed and its destruction recorded.

Table 13: *Post factum* review

Measure	**Covert communications monitoring**
Authorised by	Preliminary proceedings judge
Report submitted to	Preliminary proceedings judge
Report must contain	The start and end date of the monitoring; details of the officer who conducted the monitoring; a description of technical equipment used; the data collected and an evaluation of the operations applicability and its results.
Are materials destroyed if not used as evidence?	Yes
Is the subject informed of the operation if the materials are not used as evidence?	It is possible, but not compulsory.
Measure	**Covert tailing and recording**
Authorised by	Preliminary proceedings judge
Report submitted to	Preliminary proceedings judge
Report must contain	The same type of data as the report for covert communications monitoring
Are materials destroyed if not used as evidence?	Yes
Is the subject informed of the operation if the materials are not used as evidence?	No
Measure	**Simulated business activity**
Authorised by	Preliminary proceedings judge
Report submitted to	Preliminary proceedings judge
Report must contain	The date of simulated activity; details of the official involved (unless this was an undercover agent); a description of technical equipment used; details of those included in the operation; all documentation on the operation, including visual, audio and electronic recordings and other evidence.
Are materials destroyed if not used as evidence?	Yes
Is the subject informed of the operation if the materials are not used as evidence?	No

Measure	**Computer data search**
Authorised by	Preliminary proceedings judge
Report submitted to	Preliminary proceedings judge
Report must contain	The start and end time of the search; data searched and processes; details on the official who conducted the search; a description of technical equipment used; details on those affected by the operation.
Are materials destroyed if not used as evidence?	Yes
Is the subject informed of the operation if the materials are not used as evidence?	No
Measure	**Controlled delivery**
Authorised by	Public prosecutor
Report submitted to	Public prosecutor
Report must contain	The start and end date of the delivery; details on the official who conducted the operation; a description of technical equipment used; details on those affected by the operation.
Are materials destroyed if not used as evidence?	
Is the subject informed of the operation if the materials are not used as evidence?	No
Measure	**Engagement of an undercover agent**
Authorised by	Preliminary proceedings judge
Report submitted to	Preliminary proceedings judge
Report must contain	The start and end date of the operation; the codename or alias of the agent; a description of techniques and equipment used; details on those affected by the operation; details of results achieved. Also included are photographs, visual, audio or electronic recordings, documentation and all other evidence.
Are materials destroyed if not used as evidence?	Yes
Is the subject informed of the operation if the materials are not used as evidence?	No

Measure	**Access to phone records, base stations used or locations from which communications were conducted**
Authorised by	Preliminary proceedings judge
Report submitted to	No report is required but the police must inform the public prosecutor.
Report must contain	
Are materials destroyed if not used as evidence?	No
Is the subject informed of the operation if the materials are not used as evidence?	It is not explicitly required but the CPC provides those subject to this measure the "can file a complaint with the judge presiding over preliminary proceedings"
Measure	**Access to data from banks and other financial institutions**
Authorised by	Public prosecutor requests data directly from banks or other financial organisations.
Report submitted to	
Report must contain	
Are materials destroyed if not used as evidence?	Yes
Is the subject informed of the operation if the materials are not used as evidence?	Yes
Measure	**Monitoring suspicious transactions**
Authorised by	Preliminary proceedings judge
Report submitted to	No report is submitted.
Report must contain	
Are materials destroyed if not used as evidence?	Yes
Is the subject informed of the operation if the materials are not used as evidence?	No

LAWS ON THE SECURITY SERVICES

According to the laws on the security services (the Law on the Security-Information Agency and the Law on the Military Intelligence Agency and Military Security Agency), judicial review of measures is performed primarily *ex ante*. Furthermore, the different courts are responsible for measures that have the same fundamental purpose –

prevention of threats to the Republic of Serbia or those directed against the Ministry of Defence and the Serbian Armed Forces.

Ex Ante Review

The Security-Information Agency: Special measures infringing on the privacy of correspondence and other communications were, until amendments to the Law on the BIA in June 2014, approved by the High Court of Cassation. After these amendments the measures are approved by the President of the High Court in Belgrade, or rather a judge from the Special Department for Combating Organised Crime, as selected by the presiding judge. If the court turns down the request, the BIA Director can appeal the decision with the Appeals Court in Belgrade.

There are, however, two cases in which *ex ante* review of special measures is not possible.

Firstly, in addition to measures that infringe the privacy of correspondence, these are approved by the Agency's Director rather the courts. This includes the following[24]:

- Covert cooperation
- Covert searches of premises and objects
- Covert surveillance and monitoring

These measures are not mentioned not closely regulated by the Law on the BIA, they are regulated by secondary legislation on the BIA that is classified. As a result, there is no proper legal basis for external review of their application. That these measures are not explicitly regulated by law is all the mose surprising since their use infringes upon the right to privacy and given the fact that similar measures applied by the VBA (covert access of data records, cover surveillance and monitoring of persons in open and public spaces using technical equipment, covert recording and documentation of conversations in external and internal spaced using technical equipment) are regulated by the Law on the VBA and VIA.

The second instance, is the attendant extension of measures already approved by the courts. Specifically, if in the course of an operation the BIA becomes aware that the person subject to a special measure is using a different means of communica-

24 Security-Information Agency, response to BCSP questionnaire, Belgrade, 17/12/2014

tion, a different electronic or other address (or, for example, a different phone), the Director can order the measure to be extended. The Director of the BIA first orders the measure to be extended and only then, within 48 hours, requests court approval for the attendant extension. The court must then decide to approve the proposed extension within 48 hours of receiving the request, which means that it is possible for the BIA to apply measures that infringe on the privacy of correspondence and other communications, essentially without a court order. If the court rejects the request for attendant expansion of the measures, the data collected until that point must be destroyed in the presence of a judge. It is not, however, understood why the Director is not required to seek immediate court approval for these extensions, especially when the law makes no mention of attendant extensions being undertaken in cases of extreme urgency.

The Military Security Agency: Special evidence gathering procedures and measures defined by the Law on the VBA and VOA are subject to three approval regimes. Individual procedures and measures are approved by the Director of the VBA. The application of covert electronic monitoring of telecommunications and information systems is approved by a high court form the appeals court in the region where the measures are applied. Meanwhile, covert recording of conversations, covert access to correspondence and covert surveillance and recording inside buildings is approved by the Supreme Court of Cassation.

In urgent cases, the Director of the VBA may order the application of special procedures and measures that otherwise require court approval with the ‘consent’ of the relevant judge. Formal request for approval is submitted to the same judge within 24 hours, however, it is not quite clear what constitutes ‘consent’ and how it is recorded.

Table 14: Measures Authorised by Courts

Security Service: Measure	Approved by	Approval Period
BIA: Special measures that infringe on the privacy of correspondence and other communications	President of the High Court in Belgrade or a judge from the Special Department for Combating Organised Crime, as selected by the presiding judge	48 hours
VBA: covert electronic monitoring of telecommunications and information systems in order to access data on telecommunications traffic, without access to the content of communications	High court form the appeals court in the region where the measures are applied or where the activity took place, the detection, tracking and prevention of which is the responsibility of the VBA – approved by a judge selected by the Court President.	8 hours
VBA: covert recording of conversations in open spaces and inside buildings using technical equipment	Supreme Court of Cassation – approved by a judge selected by the President of the Supreme Court	24 hours
VBA: covert access to correspondence and other communications, including covert electronic surveillance of the content of communications and information systems	Supreme Court of Cassation – approved by a judge selected by the President of the Supreme Court	24 hours
Covert monitoring and recording inside buildings and closed spaces	Supreme Court of Cassation – approved by a judge selected by the President of the Supreme Court	24 hours

Review during Application:

Judicial review during the application of measures in accordance with laws governing the security services is not prescribed.

Table 15: Judicial review by phase of measures implementation

Service	Measure	*Ex ante* judicial review	*Post factum* judicial review
Security-Information Agency	1. Covert cooperation 2. Covert searches of premises and objects 3. Covert surveillance and monitoring	No	No
	Special measures that infringe on the privacy of correspondence and other communications: 1. Covert monitoring and recording of communications regardless of the technical means used or monitoring electronic and other addresses; 2. covert monitoring and recording of communications in public places and places access is restricted or inside premises; 3. statistical electronic monitoring of communications and information systems with the aim of gathering data on communications or the use of mobile devices; 4. computer data searches of processed personal data and comparative analysis with data gathered using measures 1-3	Yes, except in cases of attendant expansion of the measure	No
Military Security Agency	1. Operational infiltration of organisations, groups or institutions 2. Covert acquisition of documents or objects 3. Covert access to databases, in accordance with the law 4. Covert tailing and monitoring of persons in open spaces and public places using technical equipment	No	No
	1. Covert electronic monitoring of telecommunications and information systems in order to access data on telecommunications traffic, without access to the content of communications 2. Covert monitoring and recording inside buildings, closed spaces and premises	Yes	Yes (The relevant judge is informed that the measure's application has been concluded)

Post Factum Review

Security-Information Agency: Judicial review after the application of special measures infringing on the privacy of correspondence and other communications is not prescribed by law. In other words, the BIA is not required to report the judge who approved the measures on their conclusion or to submit a final report.

The only situation in which *post factum* review is exercised is the preventative application of special measures which provides evidence of a criminal offence. In such cases, the resultant materials are submitted to the relevant Public Prosecutor's Office and are handled in accordance with the CPC.

The Military Security Agency is, upon the completion of an operation for which it required judicial approval, obliged to inform the judge of the conclusion of the operation. This does not, however, have to include a report on the applied measures. As such, the judge who approved the measures can record the duration of the operation but cannot confirm that information pertaining to those persons who were subject to the measure matches information from the approval request, or any other results of the measure's application.

As with the BIA, the VBA is required to inform the relevant Public Prosecutor's Office in cases when information gathered during the application of special investigative measures points to the preparation or execution of a crime. This does not, however, have to include information on the applied measures that led to this knowledge and does not, therefore, contribute to the possibility of *post factum* review.

The National Assembly

Oversight exercised by the National Assembly is always *post factum* oversight, i.e. after the event. The law, moreover, expressly prohibits deputies requesting information from the security services pertaining to ongoing operations.

The National Assembly monitors implementation of special measures primarily through the relevant committees.

The Security Services Control Committee oversees the work of the Security-Information Agency, the Military Security Agency and the Military Intelligence Agency. The Committee is explicitly authorised to oversee the legality of the application of special procedures and measures for covert data collection.[25] In addition, the Committee monitors the services' political, ideological and interest neutrality, the legality of their expenditure of budgetary and other resources and investigates illegal or unlawful practices and adopts conclusions thereon. These powers are also significant in overseeing the application of special investigative measures.

In order to exercise oversight, the Committee has several instruments at its disposal.

The Directors of the services are required to submit regular reports to the Committee, at least once per parliamentary session. This is an opportunity for the Committee members to request comprehensive statistical data on the application of special measures.

Oversight of the legality of budgetary and other expenditure, for example, grants Committee members the right to review the legality of funds spent on covert use of property and services provided, for a fee, by individuals and businesses.

In addition to regular reports, the Committee can request that the Directors submit an unscheduled report. These reports are a useful tool for the clarification of certain issues and, potentially, ongoing scandals, regarding the implementation of special investigative measures.

25 Law on Bases of Security Service Organization, Article 16, Item 2, Point 3

*The breadth of oversight does not depend only on the legal powers of deputies but also on the way security services are structured and their internal practices when it comes to recording the use of special measures. For example, the VBA is not required by law to keep records on special data collection procedures and measures, if these have been court approved. In practice, the VBA does not keep records on the total number of annual requests made for the application of special procedures and measures, nor the number of special procedures and measures actually applied.**

* Military Security Agency, response to BCSP questionnaire, Belgrade, 05/01/2015

The Security Services Control Committee also exercises indirect oversight through oversight inspections. Members of the Committee have the right to visit the offices of the service, gain access to documentation and ask for information on the service's activities. Furthermore, the law explicitly lists the types of data National Assembly deputies cannot access[26], this includes information on:

- The identity of current and former operatives;
- The service's operatives working undercover;
- Third persons who could be endangered by their identity becoming known;
- Methods on obtaining intelligence and security-related data;
- Ongoing operations;
- Data and intelligence acquired through cooperation with foreign services and international organisations;
- Classified information and information from other state bodies held by the service.

This means that Committee members have the right to access information relating to any other aspect of the service's activities, including information classified as secret to some degree.

26 Law on Bases of Security Service Organization, Article 19, Item 2

The Inspector General of the military services monitors whether special procedures and measures for covert data collection are applied lawfully by the VBA and VOA.

The Inspector General is a body that combines the characteristics of internal and external oversight: constituted by the Government for a period of five years, it is responsible to the Minister of Defence, but it reports to the Security Services Control Committee on the implemented oversight.

In overseeing the activities of the VBA and the VOA, the Committee has legally established cooperation with the Inspector General of the military services, which submits at least one annual oversight report to the Committee.

The manner in which these oversight inspections are conducted is regulated by a Decision passed by the Security Services Control Committee during the 2012-2014 parliamentary session and re-adopted by the Committee in its current session (2014-). The Decision does not constitute a legal document, however, as neither the Law on the National Assembly nor the Rules of Procedure grant committees with the power to pass internal regulations. As a result, the Decision is not binding for committees in future convocation – each must decide to once again adopt the Decision or to regulate oversight inspections in a different manner or not to regulate them at all.

The Decision, which is currently in force, does not prescribe a method (or methods) for selection of the subject the deputies will review in the field. In practice, this reduces the predictability and effectiveness of these oversight inspections.

It is worth mentioning that the heads of the internal affairs departments at the VBA and the VOA must notify the Inspector General and, if necessary, the relevant National Assembly committee, in the event that the director of the service fails to rectify illegalities or irregularities their department has previously identified.

The Security Services Control Committee is required to take into consideration petitions regarding the security services and from ordinary members of the public and to propose measures to address issues highlighted. This allows the Committee to detect any irregularities in the implementation of special investigative measures, which could lead to it requesting an unscheduled report from the service director or, if appropriate, organising an oversight inspection.

The Defence and Internal Affairs Committee exercises oversight of the Ministry of Internal Affairs and the General Police Directorate. Unlike the Security Services Control Committee, this committee does not have any explicit powers to exercise oversight of the use of special measures by the police or, more specifically, the Criminal Force Directorate. The Committee does, however, have the power to deliberate on all issues pertaining to internal affairs, which certainly includes the application of special measures.

As the Defence and Internal Affairs Committee does not have explicit powers to exercise oversight of the implementation of special measures so the instruments at its disposal for this are quite limited. Nevertheless, by putting what instruments are available to them to good use, the committee members can still come by significant information.

The Ministry of Interior submits regular reports on its activities and the state of security. In practice, these reports have so far referred only to the security situation in Serbia and have not offered detailed information on the work of the Ministry or police methods. Even so, the Committee could use deliberation of the regular reports as an opportunity to request information on the number of evidence gathering operations and targeted searches implemented.

The Defence and Internal Affairs Committee can also request that the Minister of Interior submit unscheduled reports on "issues pertaining to their jurisdiction".

The Security Services Control Committee and the Defence and Internal Affairs Committee can also improve oversight of the application of special measures by establishing regular cooperation with independent regulatory bodies, the Ombudsman and the Commissioner for Information of Public Importance and Personal Data Protection.

The Committees, according to the National Assembly Rules of Procedure, can also engage experts in order to more closely examine issues within the jurisdiction of the National Assembly. The engagement of experts in law, technology and security could afford deputies greater insight into the application of special measures. For example, telecommunications experts could aid deputies by indicating what they should pay closer attention to when it comes to covert communications monitoring.

National Assembly deputies who are not members of either of the aforementioned committees can pose parliamentary questions on the application of special measures. They cannot gain insight into information that is classified (a right reserved for those who are members of oversight committees and the National Assembly Speaker) but they can request aggregated data on the application of measures or information on the number of training sessions members of the security services and police have attended on the application of measures.

In the event that there is a need to resolve a scandal or perceived systematic deficiency in the application of special measures, the National Assembly can establish temporary working bodies: an inquiry committee or an inquiry commission. An inquiry committee is made up of National Assembly deputies and an inquiry commission is made up of deputies, representatives of government bodies and organisations, scientists and experts. Both working bodies have the task of analysing the situation in a given area or establishing the facts about certain issues or events.

An inquiry committee or commission cannot execute investigative or other judicial activities.

An inquiry committee or commission has the right to request data, documents and information from government bodies and organisations, and can also take statements by individuals if necessary.

Representatives of government bodies and organisations are required to respond to a summons by an inquiry committee or commission and to provide truthful statements, information or documents.

Inquiry committees and commissions report, with recommendations, to the National Assembly.

The Rules on Procedure does not, however, prescribe, how an inquiry committee/commission is formed nor who can initiate its formation (how many deputies, parliamentary groups, etc.)

Independent Regulatory Bodies

Independent regulatory bodies that, within their capacity, oversee the implementation of special measures are the Ombudsman and the Commissioner for Information of Public Importance and Personal Data Protection.

The Ombudsman reviews the activities of government bodies in order to protect and promote human rights. Oversight procedure is initiated by a complaint filed by a member of the public or on the institution's own initiative. During the review process the Ombusdman has the right to access the offices of the government body – including offices of the security services – and to gather all data relevant to the review, including data classified at the highest level of secrecy ("state secret").[27] Using its far-reaching powers, **the Ombudsman's office is the only regulatory body that can review special measures during their application. In order to secure these powers the Ombudsman is required to pass rigorous security checks so as to access data classified at the highest level of secrecy ("top secret")**[28]**.**

In 2010, the Ombudsman conducted a preventative review of the Security-Information Agency.* The review included:

3. A preliminary meeting
4. A special meeting between the Ombudsman and the BIA Director
5. Review meetings
6. A clarification meeting
7. Production and presentation of a report and recommendations
8. BIA reaction to the recommendations and report on the results.

Also, during 2014, the Ombudsman conducted a review of the BIA regarding covert premises searches.** This represented a unique opportunity to review one of the special measures regulated exclusively by internal BIA regulations and is, therefore, not subject to judicial review or parliamentary oversight.

* Zaštitnik građana. „Izveštaj o preventivnoj kontrolnoj poseti Zaštitnika građana Bezbednosno-informativnoj agenciji." Del.br. 2016. Beograd, 16.10.2010.5.

** Ombudsman. Report on Review of Security-Information Agency Preparations for Covert Surveillance Measures, No. 25507, Belgrade, 03/09/204

27 Law on the Ombudsman, Official Gazette of the Republic of Serbia, Nos. 79/2005 and 54/2007, Article 21

28 Data Protection Law, Official Gazette of the Republic of Serbia, No. 104/2009, Article 38, Item 2 and Article 53

In the event that a review turns up shortcomings in the work of a government body, the Ombudsman will make recommendations on how the shortcomings can be resolved. The government body shall, no later than 60 days after receiving the recommendations, inform the Ombudsman on whether it has complied with the recommendations and resolved the shortcomings or in order to present the reasons for not complying with the recommendations.

The Commissioner has not, to date, conducted direct oversight of the application of special measures by the police, security services and the Administration for the Prevention of Money Laundering. The Commissioner has, however, twice conducted oversight of telecommunications operators that shed light on the activity of covert telecommunications surveillance: In 2011-2012 oversight was conducted of access to data stored by telephone operators, while in 2014 the subject of oversight were internet providers. The Commissioner's findings reveal weaknesses in the regulations, procedures and capabilities of the operators that lead to a risk of abuse in the application of covert telecommunications monitoring and computer data searches.

The Commissioned for Information of Public Importance and Personal Data Protection (hereafter: the Commissioner) monitors implementation of the Law on Personal Data Protection and highlights violations resulting from data collection. Since the application of special investigative measures results in the collection of personal data, this aspect of the work of security institutions is subject to oversight by the Commissioner.

The Commissioner may initiate oversight based on information that has come to their attention *ex officio*, as the result of a complaint filed by a third party. Oversight is conducted by authorised personnel, i.e. inspectors.

On the basis of results obtained in the course of oversight, the Commissioner may:

- Order the holder of the data to resolve irregularities within a given deadline;
- Temporarily prohibit the processing of data that is in contravention of the Law on Personal Data Protection;
- Order the unlawfully collected data to be deleted.[29]

29 Law on Personal Data Protection, Official Gazette of the Republic of Serbia, Nos. 97/2008, 104/2009 – Nat. Law, 68/2012 – Constitutional Court Decision and 107/2012, Article 56, Item 2

From 2014, the police, the BIA and the VBA have been required to report annually (by 31 January for the previous calendar year)[30] to the Commissioner on the number of requests for access to stored electronic data[31] they submitted to telephone and internet operators.[32] Operators are also required to submit, to the Commissioner, their own records on the number of received requests. This enables cross-referencing of access to stored data, a form of sensitive personal data. This does not, however, establish comprehensive supervision of access to stored data as the police, the BIA and the VBA are able to access data without submitting a request to the operator.

30 Which means that the police, the BIA and the VBA first submitted reports to the Commissioner on January 2015 for the 2014 calendar year.

31 Stored data are data on communications which do not reveal the content of the communications but do reveal the type of communication, the location from which it was conducted, the time the communication was conducted and who communicated with whom.

32 Law on Electronic Communications, Official Gazette of the Republic of Serbia, Nos. 44/2010, 60/2013 – Constitutional Court Decision and 62/2014, Article 130a.

WHO CAN MEMBERS OF THE PUBLIC TURN TO IF THEY BELIEVE THEIR RIGHTS HAVE BEEN VIOLATED BY THE APPLICATION OF SPECIAL MEASURES?

The first points of contact are the internal affairs departments. Members of the public can, on this level, only file complaints pertaining to the work of the police as, in the case of the BIA and the VBA, this opportunity is not explicitly legally regulated. The Law on the Police prescribes that the Internal Affairs Sector act, among other things, "on the basis of suggestions, reports and complaints filed by individuals and legal entities"*, and guarantees everyone the right to "file a complaint with the Ministry against any police official if they believe that the unlawful or improper actions of the official have violated their rights or freedoms"**. Complaints are filed with the Ministry or one of its departments in the relevant municipality in verbal, written or electronic form.*** On the other hand, the Law on the VBA and the VOA explicitly directs members of the public to the **Inspector General** of the military security services if they feel that the activities of these services have violated their human rights and freedoms.****

When it comes to independent watchdogs, members of the public can turn to the Ombudsman, which receives complaints about any government body. **The National Assembly's Security Services Control Committee** (BIA, VOA, and VBA) is empowered to "take into consideration suggestions, petitions and complaints pertaining to the security services and addressed by members of the public to the National Assembly and to propose measures for their resolution and to inform the complainant on the outcome".*****

——

* Law on the Police, Official Gazette of the Republic of Serbia, Nos. 101/2005, 63/2009 – Constitutional Court Decision and 92/2011, Article 174, Item 1

** Ibid. Article 180.

*** Rules of Procedure on Dealing with Complaints, Official Gazette of the Republic of Serbia, No. 54/2006, Article 3

**** Law on the VBA and VOA, Official Gazette of the Republic of Serbia, Nos. 88/2009, 55/2012 – Constitutional Court Decision and 17/2013, Article 61

***** Article 16 of the Law on Bases of Security Service Organization, Official Gazette of the Republic of Serbia, Nos.116/2007 and 72/2012. Same in National Assembly Rules of Procedure, Official Gazette of the Republic of Serbia No 52/10, Article 66

QUESTIONS FOR OVERSIGHT ON SPECIAL MEASURES

Questions that should be asked during the oversight process: Security-Information Agency and Military Security Agency

REQUEST REGULATIONS GOVERNING THE POLICE DEPARTMENTS APPLYING MEASURES

Suggested question:

Please provide a copy of documents regulating (1) responsibilities, (2) obligations, (3) accountability and (4) review of all activities undertaken by the Criminal Force Directorate, the Internal Affairs Sector and the Office of the Minister of Interior.

Responses to this question could yield information on how each specific department within the MoI applies special covert data collection measures and whether this area is even regulated, especially with regards to review and the prevention of misuse.

Suggested question:

Please provide a copy of documents regulating procedures for the storage of materials gathered in the application of special measures under the legal regime of the Criminal Procedure Code and the submission of said materials to the judge presiding over preliminary proceedings.

The Criminal Procedure Code does not explicitly prohibit government bodies that apply special measures from storing data and copies of materials acquired during the application of special evidence gathering activity. The courts have no way of checking that all materials have been submitted, nor whether government agencies have retained copies of, for example, visual or audio recordings, made in the course of special investigative activities, resulting in a risk of misuse. Furthermore, careless handling of materials submitted to courts leaves room for potential 'leaks'.

REQUEST STATISTICAL DATA

Suggested question:

How many times have units of the Ministry of Interior, authorised to apply special cover data collection measures according to provisions of the Criminal Procedure Code and the Law on the Police, applied these measures in previous years?

Suggested table for recording responses:

Measure	2013	2014	2015
Monitoring of suspicious transactions			
Covert communications monitoring			
Simulated business activity			
Computer data searches			
Controlled delivery			
Engagement of undercover agent			
Access to phone records, base stations used or locations from which communications were conducted			
Police observation			
Targeted search			
mere ciljanje potrage			

1. *To what extent the principle of proportionality is respected – that is, that information on a criminal offence cannot have been uncovered in another way that does not infringe on human rights – in the application of measures for covert data collection, especially in comparison with the application of 'ordinary' evidence gathering.*

2. *Whether the police keep regular annual records of special measures applied.*

3. *Which special measures are not made use of? For example, research by BCSP has shown that the special evidence gathering through engagement of undercover agent has not been approved once during the October 2013 to October 2014 period in the regions covered by 11 high courts. This begs the question, why is this meas-*

ure not in use? Does the MoI department for undercover agents have sufficient human and material resources? Do police officials receive sufficient training in the engagement of undercover agents? Can the MoI protect undercover agents during and after their operations?

CHECK THE DURATION OF APPLIED MEASURES

Suggested question:

How long does the application of measures for covert data collection, according to provisions of the Criminal Procedure Code, the Law on the Police and the Law on Electronic Communications, last on average in accordance with standard police practice?

Suggested table for recording responses:

Measure	Duration	Legal restriction
Monitoring of suspicious transactions		Three months, with possibility to be extended three times by a further three months.
Covert communications monitoring		3 months, which can be extended by a further 3 months a maximum of three times
Covert tailing and recording		3 months, which can be extended by a further 3 months a maximum of three times
Simulated business activity		3 months, which can be extended by a further 3 months a maximum of three times
Computer data search		3 months, which can be extended by a further 3 months a maximum of three times
Controlled delivery		Until the package is delivered
Engagement of undercover agent		3 months, which can be extended by a further 3 months a maximum of three times
Access to phone records, base stations used and locations from which communications were conducted		3 months, which can be extended by a further 3 months a maximum of three times
Police observation		Unlimited
Targeted search		Six months, which can be extended by further six months

Based on responses to this question you can check and confirm whether legal constraints on the application of special covert data collection measures are observed, as well as whether the application of special measures is effective – if they are always ap-

plied for the maximum permitted duration this is likely not a good sign either for police effectiveness nor for human rights.

LOOK INTO THE WORK OF THE INTERNAL AFFAIRS SECTOR

Suggested question:

How many times has the Police Internal Affairs Sector pressed for criminal charges or proposed disciplinary proceedings against police officers for misuse of data obtained through the application of measures for covert data collection?

Based on responses you can check and confirm what the Internal Affairs Sector does to prevent and investigate, for example, 'information leaks' from the police and the data collected in the application of covert data collection measures. To follow up you can check whether sanctions for misuse are prescribed as, according to the Law on the Police, the disclosure to unauthorised persons of confidential information as defined by law and other regulations is a serious breach of official duty.

LEARN WHAT PROBLEMS EXIST

Suggested question:

What special data collection measures can the police apply independently, without resorting to use of BIA technical capabilities?

What training courses on the application of special covert data collection measures do police officers attend? Who runs these training courses?

Based on responses to these questions you can discover which technical, material and human resource problems the police face in applying special covert data collection measures. Responses to the first question can form the basis for further investigation of why the police rely in BIA resources. This is not in line with best practices established by EU member states. From responses to the second question you can learn how determined the MoI is to improve its employees' ability to apply special measures in accordance with principles of human rights.

Suggested question:

How many requests for access to stored data have been sent to telecommunications operators over the past year? How many times have stored data been accessed, with or without the consent of the operators?

The police are able to access data on members of the public at any time, they do not need operator approval. Operators have the technical ability to register every time stored on their users data are accessed but are required by law to keep records only of the number of requests they have received. The police are also required to keep records only on the number of requests submitted and to report these records to the Commissioner for Information of Public Importance and Personal Data Protection, on an annual basis. This means that access to stored data gained without a formal request is currently an external oversight 'blind spot'.

Suggested question:

Could you please specify all types of stored data the police have gained access to. Are websites the user has visited included in these data?

The types of data stored are defined by the Law on Electronic Communication.[33] *Nevertheless, the way they are defined is much more appropriate for telephone rather than internet traffic. Further regulation on stored data should come from a rulebook on technical requirements for lawful interception of electronic communications and access to stored data, which the Ministry of Trade, Tourism and Telecommunications has yet to adopt. Website views are a particularly problematic type of data because, although at first glance they appear to be stored data, they actually reveal the content of communications.*

33 Law on Electronic Communications, Article 129

Questions that should be asked during the oversight process: Security-Information Agency and Military Security Agency

REQUEST REGULATIONS GOVERNING THE POLICE DEPARTMENTS APPLYING MEASURES

Suggested question:

Please could you provide the regulation that governs the application of covert data collection measures approved by the Director of the Agency?

The Security-Information Agency: Research by BCSP shows that the BIA applies three special measures on the basis of a classified internal regulation. The measures are covert searches of premises and objects, covert cooperation and covert surveillance and monitoring. *It is important, therefore, to learn how the application of these measures is regulated and whether their use is determined by the principle of proportionality. At any event, as long as the measures are governed only by secret internal regulations there is no predictability; i.e. the public do not know under what circumstances they may be subject to covert searches nor in which kinds of premises these searches can be applied. This is why it is important, in the long run, that the application of covert data collection measures be specifically governed by law.*

The Military Security Agency: The application of special procedures and measures for covert data collection should, according to the law, be closely regulated by the Minister of Defence, on proposal by the Director of the VBA and with the involvement of the National Security Council. The Minister of Defence also regulates the means and conditions for determining fees for covert cooperation with persons or legal entities.[34]

Suggested question:

Please could you provide a copy of the document that regulates procedures for the storage and submission to the preliminary proceedings judge of data acquired in the application of special measures, according to provisions of the Criminal Procedure Code.

34 Law on the Military Security Agency and the Military Intelligence Agency, Article 22

The Criminal Procedure Code does not explicitly prohibit the government bodies that apply evidence gathering measures from storing data and copies of materials acquired in the application of said measures. Courts do not have any way of checking whether they are in receipt of all materials or whether the government agencies have retained copies, for example, of visual or audio recordings made in the course of special investigative activities, resulting in a risk of misuse. Furthermore, careless handling of materials submitted to courts leaves room for potential 'leaks'.

REQUEST STATISTICAL DATA

Suggested question:

How many times, in previous years, has the Agency[35] been authorised to apply covert data collection measures according to provisions of the Criminal Procedure Code?

Suggested table for recording responses:

Measure	2013	2014	2015
Monitoring of suspicious transactions			
Covert communications monitoring			
Covert tailing and recording			
Simulated business activity			
Computer data searches			
Controlled delivery			
Engagement of undercover agent			
Access to phone records, base stations used or locations from which communications were conducted			

35 BIA or VBA

For the BIA

Could you please specify the number of requests, for the application of special measures that violate the right to private correspondence and other communications, the Director of the Agency has submitted to the courts over the past year? How many requests were rejected? What reasons were given for the rejection of requests?

Suggested table for recording responses:

Measure	Total number of requests submitted to the courts during ____ (year)	Number of approved requests	Number of rejected requests
Covert surveillance and recording of communications regardless of the technical means used or monitoring of electronic or other addresses			
Covert surveillance and recording of communications in public places and places where access is restricted or inside premises			
Statistical electronic monitoring of communications and information systems with the aim of gathering data on the communication or the location in which a mobile device was used			
Computer data searches of already processes personal and other data			

How many times, in previous years, has the Director of the Agency or a person authorised by the Director issued a warrant for the application of the following measures:

- Covert search or premises and objects
- Covert cooperation
- Covert surveillance and monitoring?

For the VBA

Please could you specify the number of requests for the application of special data collection procedures and measures the Director of the Agency has submitted to the courts over the past year? How many requests were rejected? What reasons were given for the rejection of requests?

Suggested table for recording responses:

Measure	Total number of requests submitted to the courts during ____ (year)	Number of approved requests	Number of rejected requests
Statistical electronic monitoring of communications and information systems with the aim of gathering data on communications traffic without accessing the content of communications			
Covert recording and documentation of conversations in open or closed spaces using technical equipment			
Covert monitoring of the content of correspondence and other communications, including covert electronic monitoring of the content of communications and information systems			
Covert monitoring and recording within premises, closed spaces and objects			

How many times, in previous years, has the Director of the Agency or a person authorised by the Director issued a warrant for the application of the following measures:

1. Operational infiltration of organisations, groups and institutions;
2. Covert acquisition of documents and objects;
3. Covert access of records, in accordance with the law;
4. Covert tailing and monitoring of persons in open spaces, public places with use of technical equipment;
5. Covert use of services provided by persons or business for a fee.

Based on responses to these questions, you can learn:

1. *How frequently the BIA/VBA propose the use of special measures. This enables the tracking of trends from year to year and forms a basis for the formulation of further questions on whether measures are applied appropriately. The Law on the BIA requires that decisions on the application of measures take into account whether the same results could be achieved by means less restrictive to the rights of the public[36]. This is an important question that should be taken into consideration as a matter of course when reviewing the application of special measures.*
2. *How frequently courts reject requests for the application of measures and why.*
3. *Whether and how thoroughly the security services keep records on the proposal and application of special measures.*
4. *What the relationship is between operations and the use of covert communications monitoring, which has a greater impact on the privacy of members of the public? Is covert communications monitoring used as a substitute for operations and how is this justified?*

Suggested question:

How long does the application of measures for covert data collection, according to provisions of the Criminal Procedure Code and the Laws on the BIA/VBA/VOA, last on average?

Suggested table for recording responses:

Measure	Duration	Legal restriction
Criminal Procedure Code		
Monitoring of suspicious transactions		Three months, with possibility to be extended three times by a further three months.
Covert communications monitoring		3 months, which can be extended by a further 3 months a maximum of three times
Covert tailing and recording		3 months, which can be extended by a further 3 months a maximum of three times
Simulated business activity		3 months, which can be extended by a further 3 months a maximum of three times
Computer data search		3 months, which can be extended by a further 3 months a maximum of three times

36 Law on the Security-Information Agency, Article 14

Controlled delivery		Until the package is delivered
Engagement of undercover agent		3 months, which can be extended by a further 3 months a maximum of three times
Access to phone records, base stations used and locations from which communications were conducted		3 months, which can be extended by a further 3 months a maximum of three times
Law on the Security-Information Agency		
Covert surveillance and recording of communications regardless of the technical means used or monitoring of electronic or other addresses		3 months, which can be extended by a further 3 months a maximum of three times
Covert surveillance and recording of communications in public places and places where access is restricted or inside premises		3 months, which can be extended by a further 3 months a maximum of three times
Statistical electronic monitoring of communications and information systems with the aim of gathering data on the communication or the location in which a mobile device was used		3 months, which can be extended by a further 3 months a maximum of three times
Computer data searches of already processes personal and other data		3 months, which can be extended by a further 3 months a maximum of three times
Law on the Military Security Agency and the Military Intelligence Agency		
Statistical electronic monitoring of communications and information systems with the aim of gathering data on communications traffic without accessing the content of communications		Six months, which can be extended by further six months
Covert recording and documentation of conversations in open or closed spaces using technical equipment		Six months, which can be extended by further six months
Covert monitoring of the content of correspondence and other communications, including covert electronic monitoring of the content of communications and information systems		Six months, which can be extended by further six months
Covert monitoring and recording within premises, closed spaces and objects		Six months, which can be extended by further six months

Based on responses to these questions you can check and confirm whether legal restrictions on the duration of covert data collection measures are respected, as well as how effective the measures are – if they are always applied for the maximum permitted duration this is likely not a good sign either for the service's effectiveness nor for human rights.

CHECK WHAT THE SECURITY SERVICE'S PRIORITIES ARE IN APPLYING MEASURES.

Suggested question:

Please name the five criminal offences for the investigation of which the Agency has most frequently applied covert data collection measures (special investigative activity) over the past year.

Based on responses to this question you can learn what the greatest security threats are in Serbia and compare them with external analysis of challenges, risks and threats. The responses will also indicate the priority areas for the Agencies. This can form the basis of additional questions on the justifiability of the Agencies dealing with these threats.

For the BIA: For the previous year, what percentage of measures were applied according to the Criminal Procedure Code and what percentage were applied according to the Law on the BIA?

For the VBA: For the previous year, what percentage of measures were applied according to the Criminal Procedure Code and what percentage were applied according to the Law on the VBA and VOA?

Based on responses to these questions you can learn how frequently the BIA/VBA apply special measures preventatively (to thwart threats to the security of Serbia, the Ministry of Defence and the Serbian Armed Forces) and how often these measures are applied as part of criminal investigations. This relationship may indicate which activities the security services prioritise. Tracking this relationship from year to year should indicate how the priorities of the security services have changed and beg the question of why they have changed.

CHECK TO WHAT EXTENT THE REVIEWED SECURITY SERVICE IS CAPABLE OF INTERNALLY DETECTING AND RESOLVING ABUSES.

Suggested question:

How many times has the Internal Affairs Department brought criminal charges or disciplinary action against members of the Agency regarding abuse of powers in applying measures for covert data collection?

Based on responses to this question it is possible to assess the capability of the reviewed service to internally resolve problems relating to abuse of powers. Responses may also lead to additional questions about the capacities of internal affairs departments and their position within the services.

LEARN WHAT PROBLEMS EXIST

Suggested question:

What training do operatives of the Agency receive on the application of special covert data collection measures? What does the training focus on?

Training received by members of the security services on special measures does not necessarily guarantee that they know how to apply these measures lawfully and without unduly infringing on the rights of members of the public. The Ombudsman's 2014 report on a review of the BIA's application of covert surveillance measures highlighted the need to train personnel so as to prevent unlawful infringement, through ignorance or carelessness, of people's rights[37].

Suggested question:

How many requests for access to stored data have been submitted to telecommunications operators over the past year? How many times have stored data been accesses successfully, with or without submission of a request to the operators?

37 Ombudsman, Review of the Security-Information Agency's Application of Covert Surveillance Measures. No. 614-506/14. Belgrade, 03/09/2014: p. 5

The BIA and VBA are able to access data on members of the public at any time, they do not need operator approval. Operators have the technical ability to register every time stored on their users data are accessed but are required by law to keep records only of the number of requests they have received. The police are also required to keep records only on the number of requests submitted and to report these records to the Commissioner for Information of Public Importance and Personal Data Protection, on an annual basis. This means that access to stored data gained without a formal request is currently an external oversight 'blind spot'.

Suggested question:

Could you please specify all types of stored data the Agency has accessed. Are websites the user has visited included in these data?

The types of data stored are defined by the Law on Electronic Communication. Nevertheless, the way they are defined is much more appropriate for telephone rather than internet traffic. Further regulation on stored data should come from a rulebook on technical requirements for lawful interception of electronic communications and access to stored data, which the Ministry of Trade, Tourism and Telecommunications has yet to adopt. Website views are a particularly problematic type of data because, although at first glance they appear to be stored data, they actually reveal the content of communications.

Questions for the high courts[38]

How many times during _____ (year) have judges presiding over preliminary proceedings rejected requests for the application of special investigative activity and other covert data collection measures prescribed by the Criminal Procedure Code?

What are the most common ground, based on Serbian jurisprudence, for the rejection by a preliminary proceedings judge of a request to apply special investigative activity and other covert data collection measures prescribed by the Criminal Procedure Code?

From responses to these questions it will be possible to learn which irregularities typically arise in the application of special measures and how frequent they are.

How many times during _____ (year) have judges presiding over preliminary proceedings approved requests by public prosecutors to destroy material collected through special investigative activity and other covert data collection measures prescribed by the Criminal Procedure Code?

What are the common grounds on which a preliminary proceedings judge issues a decision on the destruction of collected materials?

From responses to these questions it will be possible to learn how frequently applied measures do not achieve their desired aims (gathering evidence) and why this is the case.

How much and what kind of training have judges received to date regarding the approval of special investigative activity and other covert data collection measures prescribed by the Criminal Procedure Code?

Well trained judges are indispensible for the lawful approval of special investigative activity and other covert data collection measures prescribed by the Criminal Procedure Code.

---

38 Questions that should be posed by civil society organisations, in other words, the interested public. Parliamentary oversight focuses on the executive authority: the Ministry of Interior, the Ministry of Defence and the security services.

Questions for the higher public prosecutor's offices[39]

How many times during _____ (year) have courts dismissed evidence submitted by the prosecutor's office due to it being gathered unlawfully through special investigative activity and covert data collection measures.

From responses to these questions it will be possible to establish how frequently special investigative activity is conducted unlawfully but also how effectively these measures are applied – if special investigative activity is not applied in accordance with the law, it does not result in quality evidence. Thus, the rights of the public are violated 'at their expense'.

How much and what kind of training have public prosecutors received to date regarding the approval of special investigative activity and other covert data collection measures prescribed by the Criminal Procedure Code?

Well trained public prosecutors are indispensible for the lawful and effective proposal and selection of special investigative activity and other covert data collection measures prescribed by the Criminal Procedure Code.

39 See above footnote.

LEGAL FRAMEWORK

- "The Constitution of the Republic of Serbia" Official Gazette of the Republic of Serbia, No. 98/2006
- "Law on the Security-Information Agency" Official Gazette of the Republic of Serbia, Nos. 42/2002, 111/2009, 65/2014 – Constitutional Court Decision and 22/2014
- "Law on Detective Activity" Official Gazette of the Republic of Serbia, No. 104/2013
- "Law on Electronic Communications" Official Gazette of the Republic of Serbia, Nos. 44/2010, 60/2013 – Constitutional Court Decision and 62/2014
- "Law on the Bases of Security Services Organization" Official Gazette of the Republic of Serbia, Nos. 116/2007 and 72/2012
- "Law on the Police" Official Gazette of the Republic of Serbia, Nos. 101/2005, 63/2009 – Constitutional Court Decision and 92/2011
- "Law on the Military Security Agency and the Military Intelligence Agency" Official Gazette of the Republic of Serbia, Nos. 88/2009, 55/2012 – Constitutional Court Decision and 17/2013
- "Criminal Procedure Code" Official Gazette of the Republic of Serbia, Nos. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013 and 55/2014
- "Law on the Prevention of Money Laundering and Financing of Terrorism" Official Gazette of the Republic of Serbia, Nos. 20/2009, 72/2009 and 91/2010
- "Law on Classified Information" Official Gazette of the Republic of Serbia, No. 104/2009
- Law on Personal Data Protection, Official Gazette of the Republic of Serbia, Nos. 97/2008, 104/2009 – state law, 68/2012 – Constitutional Court Decision and 107/2012
- Law on the Ombudsman, Official Gazette of the Republic of Serbia, Nos. 79/2005 and 54/2007

- "Rules of Procedure of the National Assembly of the Republic of Serbia" Official Gazette of the Republic of Serbia, Nos. 52/2010 and 13/2011
- National Assembly of the Republic of Serbia – Security Services Control Committee "Decision Regulating Direct Oversight of the Security Services in Accordance with the Law Regulating the Basic Organisation of the Security Services of the Republic of Serbia, the Laws on the Security Services and the Rules of Procedure of the National Assembly. Number 02-1322/13" Belgrade, 29 March 2013.